A hierarchical methodology for verifying microprogrammed microprocessors

P.J. Windley

To date, several microprocessors have been verified using formal methods. The only successful verification efforts, however, have been on relatively simple microprocessor architectures (fewer than 32 words of micro instruction store, small instruction set, limited features for supporting operating systems, etc.). The goal of the research reported is to develop methodologies for verifying much larger architectures and demonstrate their applicability verifying such a microprocessor. A hierarchical methodology is presented for decomposing microprocessor verifications which reduces the necessary effort by more than an order of magnitude. A secondary result of the research is a verified microengine that can be used to quickly implement verified microprocessors with varied architectures.

Privacy-enhanced electronic mail

M. Bishop

The security of electronic mail sent through the internet may be described in exactly three words: there is none. The Privacy and Security Research Group has recommended implementing mechanisms designed to provide security enhancements. The first set of mechanisms provides a protocol to provide privacy, integrity and authentication for electronic mail; the second provides a certificate-based key management infrastructure to support key distribution throughout the internet, to support the first set of mechanisms. This paper describes these mechanisms, as well as the reasons behind their selection and how these mechanisms can be used to provide some measure of security in the exchange of electronic mail.

Towards a testbed for malicious code detection

R. Lo, P. Kerchen, R. Crawford, W. Ho, and others

An environment for detecting many types of malicious code, including computer viruses, Trojan horses, and time/logic bombs, is proposed. The malicious code testbed (MCT) is based upon both static and dynamic analysis tools developed at the University of California, Davis, which have been shown to be effective against certain types of malicious code. The testbed extends the usefulness of these tools by using them in a complementary fashion to detect more general cases of malicious code. Perhaps more importantly, the MCT allows administrators and security analysts to check a program before installation, thereby avoiding any damage a malicious program might inflict.

Secure computation

S. Micali, P. Rogaway

The authors define what it means for a network of communicating players to securely compute a function of privately held inputs. Intuitively, they wish to correctly compute its value in a manner which protects the privacy of each player's contribution, even though a powerful adversary may endeavor to disrupt this enterprise. The definition is built on several new ideas. Among them: Closely mimicking an ideal evaluation. A secure protocol must mimic this abstraction in a run-by-run manner, our definition depending as much on individual executions as on global properties of ensembles. Blending privacy and correctness in a novel way, using a special type of simulator designed for the purpose. Requiring adversarial awareness-capturing the idea that the adversary should know, in a very strong sense, certain information associated to the execution of a protocol. Among the noteworthy and desirable properties of definition is the reducibility of secure protocols, which is a cornerstone in a mature theory of secure computation.